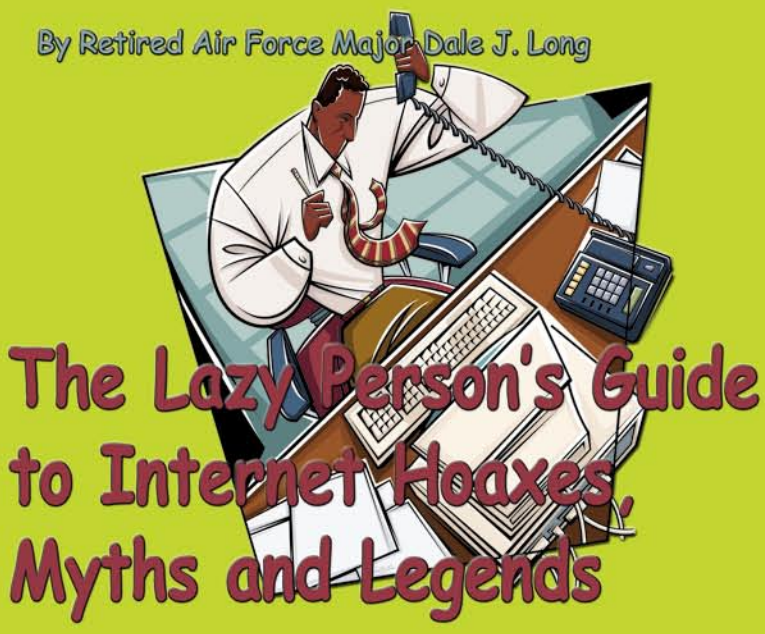
By Retired Air Force Major Dale J. Long



The Lazy Person's Guide to Internet Hoaxes, Myths and Legends

Urgent! Urgent! All Cell Phone Users!

From: Zippy
Sent: December 01, 2004 10:08
To: All of my friends
Subject: FW: IMPORTANT!

Starting Jan. 1, 2005, all cell phone numbers will be made public to telemarketing firms. So this means as of Jan. 1, your cell phone may start ringing off the hook with telemarketers, but unlike your home phone, most of you pay for your incoming calls. These telemarketers will eat up your free minutes and end up costing you money in the long run.

According to the National Do Not Call List, you have until Dec. 15, 2004, to get on the national "Do not call list" for cell phones. Registering only takes a minute. Make sure you register now!

Figure 1.

You are traveling through another dimension — a dimension of bits and bytes and information. It is a journey into a wondrous land whose boundaries are that of imagination and there is a signpost up ahead. Your next stop: the Internet Zone. Within the vast, bright realm of cyberspace, however, lurk various tricksters and scam artists ranging from amusing to annoying or downright dangerous.

These miscreants have turned their not inconsiderable talents to creating stories that convince the unwary to spread the seeds of their imaginations around the world. Submitted for your consideration are some of the stories that have become Internet legends and urban myths. All of them are hoaxes, but they cling to their odd half-lives through a combination of cunning, persistence and their ability to draw new believers to their cause.

If an informed electorate is the foundation of democracy, then informed users should be the foundation of the Internet. In this issue, we will dissect a few of these hoaxes with a view to helping prevent their spread in the future. The more people who understand how chain spam really works, that there aren't really people in Nigeria who want you to launder money for them and that apparently friendly warnings usually start out as misanthropic attempts to stir up a cloud of e-mail activity, the better off we will be.

Forward Me!

What prompted this particular topic was an e-mail mass mailed by someone at one of our field offices. It went something like the message in Figure 1. Some of you may recognize this one. Zippy received it from a well-meaning person and forwarded it to another few hundred people, some of whom managed to forward it to others in the 10 minutes it took me to send a notice telling people to ignore the message because it was a hoax.

How do we know it is a hoax? On the surface, there is a grain of truth in the story. Yes, there is a National Do Not Call Registry where people can register their phone number to avoid telemarketing calls. Yes, there is an industry group trying to establish a 411 directory of cell phone numbers. Add in that many people do not trust telemarketers or telecommunications companies to protect their privacy and you have rich fertilizer to sprout a bumper crop of panicky e-mails.

However, it is just fertilizer because the main assertions are simply not true. First, there is no deadline for registering on the Do Not Call Registry. Second, current Federal Communications Commission (FCC) regulations prohibit telemarketers from calling cell phones. Finally, the industry-sponsored wireless 411 directory, as currently proposed, will only include the cell phone numbers of people who voluntarily add their numbers to the listing.

The industry group is also fighting pending legislation that would regulate cell phone directories and make it virtually impossible to create or distribute any list without voluntary participation by cell phone users. Apparently, there is enough valid information in the message to convince many otherwise rational people that this is a real problem, and they should forward the warning on to all their friends and relations as a public service. Unfortunately, all that does is encourage hackers who rely on social engineering to create even more entertaining e-mail fiction.

Other popular e-mail subjects over the past few years have been:

√ You can get free cash (or beer) by forwarding an e-mail message
√ The U.S. Postal Service is going to start collecting a 5-cent fee for every e-mail message sent
√ Business travelers are waking up in their hotel rooms in ice-filled bathtubs minus a kidney
√ Gas pump handles trapped with hypodermic needles are ready to prick you when you grab the handle (similar to ATM deposit envelopes laced with cyanide)
√ Nike will give you new shoes if you turn in your old ones
√ Money will be donated to charity (injured child, abandoned puppies, political campaign, etc.) for forwarding an e-mail
√ Pending legislation will require all gun owners to list their guns on their income tax returns
√ Your free e-mail service will cancel your account if you do not forward this e-mail

Frankly, I do not care about the subject of a chain-forwarded e-mail; I delete virtually all of them. I will admit to passing on the one about the soldier in the shack on Christmas Eve, and every once in a while I see something particularly humorous that I just have to share with a few friends. Even some that appear to be *good spam* are self-serving attempts to generate e-mail traffic. And given the proven ability of e-mail to carry malicious viruses, I am not inclined to be forever known among my friends as "Typhoid Dale" because I sent a virus to everyone in my address book.

Out of Africa

Another persistent e-mail scam that I still see in my inbox, despite a pretty good Bayesian filter, is known as the Nigerian Scam. These types of scams are known as advance fee fraud scams or 4-1-9 fraud. 419 is the number of the section of the Nigerian penal code that addresses fraud schemes.

This scam starts when you receive an e-mail plea from an allegedly wealthy foreigner, who needs your help to move millions of dollars from his homeland to the United States and will reward you with a hefty percentage of the money. Or you have won a foreign lottery you did not know you entered. Or some wealthy repentant sinner wants to leave your church millions of dollars in his will. All you have to do is send several thousand dollars in processing fees to release the money so they can send it to you.

Now you would think that upon reading this particular pitch the frontal lobes of the average cerebellum would be screaming, "WARNING, WARNING! Danger Will Robinson! SCAM, SCAM!" It is so obviously a scam that three blind hedgehogs living inside a padlocked canvas mail sack should be able to see it coming.

However, a 2002 U.S. Secret Service report (http://www.secretservice.gov/alert419.shtml) estimates that advance fee schemes still con people out of hundreds of millions of dollars every year. Advance fee scams are not new. They have been around since the Spanish Prisoner letter scam in the 1920s. But for some reason, people really want to believe in free money and, once hooked, will not let go of the illusion until they run out of money. The stories of people duped by these schemes are legion. You can find clues that you may be dealing with a hoax at the Department of Energy's Computer Incident Advisory Capability (CIAC) on its HoaxBusters site at http://HoaxBusters.ciac.org/.

Phishing Phollies

Speaking of fish, no discussion of online scamming would be complete without a description of *phishing*. This occurs when scammers "fish" for information by posing as banks, credit card companies or online businesses and try to obtain account details and pin numbers.

Most phishing today is done via e-mail. You get an official-looking e-mail from companies like Visa, Amazon.com, eBay, Smith Barney, etc., that asks you to click on an embedded link to *their* Web site and confirm your account data. While these links may appear genuine, the underlying URL (Uniform Resource Locator) in the page code takes you to the scammer's site, which is designed to look exactly like the genuine article. Once you enter your account information into the login form, you get a reassuring message that everything is just fine with your account and the scammer gets your account details.

As with advance fee scams, phishing is not new, it is based on old telephone scams where someone called up claiming to be from the bank or credit card company and asked people to *verify* their card number, expiration date, billing address, Social Security Number, etc.

Phishing has apparently been very profitable for phishers. In the United States alone, banks reportedly paid out more than $1.2 billion last year due to phishing scams. There have been reports of phishing operations that targeted a favorite phisher target: Microsoft's Internet Explorer browser. Security experts identified vulnerabilities in IE Version 6 (including those on computers updated with Windows Service Pack 2) that allowed phishers to create realistic looking Web sites that fake Secure Socket Layer signature padlock certificates and hijack cookies from other Web sites, including those with login and account information.

While it is likely that these holes will have been patched by the time you read this, browser and e-mail vulnerabilities represent the main chinks in our armor that phishers and other malicious software authors have targeted recently.

The next wave of Internet-related scams, however, may move from phishing to *pharming*. While phishing is a social attack where the scammer throws out bait and hopes someone will nibble, pharming is more like sowing seeds and waiting for them to sprout and bear fruit. Pharming involves spreading a worm or virus to host computers that automatically and invisibly redirects your browser when you try to reach a particular URL.

As users become harder to dupe with phishing schemes, we may see a shift from phishing to pharming. While all alleged reports of this form of exploitation have so far involved redirects to advertising sites, it is theoretically possible that pharming worms could become sophisticated enough to allow scammers to create a look-alike site intended to steal account information and send out instructions to their worms to redirect you from your online banking or shopping site to theirs.

Apparently, it isn't happening yet, but it may only be a matter of time. It was not so long ago that we thought you could not get a computer virus from simply opening e-mail, so I have every expectation that someone will figure out how to make pharming work, too.

Another theoretical variation on pharming is based on Domain Name System poisoning. This occurs when the scammer confuses your DNS server into believing that the site you want is an Internet Protocol (IP) address that belongs to the scammer, not the site's actual numeric address. Most Internet services rely on DNS, which is a distributed Internet directory service that has two primary functions: (1) translate between domain names and IP addresses and (2) control e-mail delivery.

In particular, Web browsers depend on DNS to locate Web sites. While your browser shows you the text-based URL, the site that

actually resolves is based on the numeric IP address, whether or not it is really the correct address. However, DNS servers do not always authenticate the source of the numeric IP address. In many cases, there is no way for a DNS server to be sure that the address actually came from the real site.

Plugging identification and authorization exploits like DNS poisoning can be a never-ending arms race with the DNS server constantly on the defensive. As with any security scheme, proper configuration of your system is crucial. If all DNS servers were configured using something similar to Secure Shell architecture, DNS poisoning or any similar scam that depends on trust-based vulnerabilities would be less of an issue. For more information, see the Internet Engineering Task Force Web site at http://www.ietf.org/html.charters/secsh-charter.html.

Mom Was Right

Of course, no amount of armor will protect anyone who insists on repeatedly swimming in shark-infested waters. There are some steps you can take to protect you from online scams, and they sound a lot like advice mom gave us when we were children:

1. Don't touch that — you don't know where it's been. Or in the case of embedded links in unsolicited e-mails, where it is going. Never click on an embedded link in spam e-mail. At best, it tells the spammer that your address is "live." At worst, it loads some type of *malware* (malicious software) on your PC that burrows in and does ugly things. If you get a message saying you need to go to your online bank, eBay account or credit card company, type the URL in yourself.

2. Don't mess around with things you don't know anything about. This one is good advice for any e-mail attachment, particularly since clever, inventive people have found ways to embed viral code in everything from word processing documents to graphics files.

3. Lock your doors. In this case, turn off or restrict anything that could be used to allow unauthorized code into your system. That includes ActiveX controls, the Windows Scripting Host and HTML rendering in e-mail.

If you are really concerned about Web vulnerabilities, you may wish to replace MS Internet Explorer with another browser. In Zippy's case, he is only safe because his wife restricts him to an old Macintosh IIsi running Mac OS version 6.7 and an ancient version of Netscape. Many people would consider that security overkill, but you were not there when Zippy tried to buy into a fake scam for Millennium Bug Insurance a few years ago (see http://www.chips.navy.mil/archives/99_jul/dale.htm for the details). His wife has not let him play on the Web by himself since.

4. Don't talk to strangers. Particularly strangers offering you free candy, money, beer or lunch online. This also applies to chat rooms, as malicious software can apparently be spread via chat software.

I got a first-hand look at this a couple of years ago when my martial arts instructor, a man with eight black belts, who owns more handheld weapons than he has ball-point pens, got cyber-mugged in a chat room by someone who hacked his computer remotely through the chat software and took control of the PC.

The only sure way to regain control after an attack like that is to physically disconnect the power, unplug the Internet connection, exorcise the offending malware by backing up the data files, reformatting the hard drive, and reloading the operating system and applications from scratch. Chat rooms are the cyberspace equivalent of hanging out in bars. If you want to be safe, go with people you know, and do not play games for money with strangers.

5. Wear your raincoat. A properly configured firewall or Web proxy (or both) can save you a lot of grief. In particular, you should have something set up to prevent unwanted intrusion and restrict what your computer might try to send out without your knowledge. Some phishing scammers do not care if you voluntarily provide them with your ID and password as long as they can download, install and activate a keystroke logger on your computer. While it may be useful to set your computer to automatically check for and download updates for your operating system or applications, you should control any activity that transmits data from your computer.

Grains of Sand and Salt

I would like to reiterate that there is a kernel of truth at the core of every successful scam. Without some veneer of credibility, people would be less likely to fall for them. The only way to combat them is with a healthy distrust of anything that shows up uninvited, regardless of how lucrative, alluring or even patriotic it seems.

If you are interested in e-mail hoaxes, scams or urban legends, there are Internet sites that are useful to those of us trying to keep Zippy from increasing the amount of junk e-mail traffic clogging the Internet.

Please e-mail this article to all of your friends. If everyone passes this on to 10 other people, eventually the entire world will read it, and we could eliminate forwarded e-mail spam forever! Then again, maybe you should just tell your friends to read the article in *CHIPS* or on the *CHIPS* Web site!

Until next time, Happy Networking!

Long is a retired Air Force communications officer who has written regularly for CHIPS since 1993. He holds a Master of Science degree in Information Resource Management from the Air Force Institute of Technology. He is currently serving as a telecommunications manager in the U.S. Department of Homeland Security.

Editor's Note: The Department of the Navy Chief Information Officer (DON CIO) offers an Information Literacy Toolkit on compact disc for use by government, industry and academia partners in support of government. The disc provides information on how users can become skilled in recognizing valid information on the Internet and in e-mail. There is also information about hoaxes online in the Exploring Online/Evaluating Information section. Go to http://www.doncio.navy.mil/iltoolkit/ for assistance. Navy NMCI users who receive unauthorized e-mail should contact the NMCI Help Desk at 1-866-843-6624 for assistance. Other government users should follow your agency's guidance on handling chain and scam e-mail. CHIPS